# REPORT DOCUMENTATION PAGE

*Form Approved*
*OMB No. 0704-0188*



| 1. REPORT DATE *(DD-MM-YYYY)* | 2. REPORT TYPE | 3. DATES COVERED *(From - To)* |
|---|---|---|
| 31-10-2008 | FINAL | |

**4. TITLE AND SUBTITLE**

The Power of Mass: Collaboration for a Netted Force

**5a. CONTRACT NUMBER**

**5b. GRANT NUMBER**

**5c. PROGRAM ELEMENT NUMBER**

**6. AUTHOR(S)**

Nancy A. Norton

Paper Advisor (if Any): CDR Ron Oard

**5d. PROJECT NUMBER**

**5e. TASK NUMBER**

**5f. WORK UNIT NUMBER**

**7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)**

Joint Military Operations Department
Naval War College
686 Cushing Road
Newport, RI 02841-1207

**8. PERFORMING ORGANIZATION REPORT NUMBER**

**9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)**

**10. SPONSOR/MONITOR'S ACRONYM(S)**

**11. SPONSOR/MONITOR'S REPORT NUMBER(S)**

**12. DISTRIBUTION / AVAILABILITY STATEMENT**

Distribution Statement A: Approved for public release; Distribution is unlimited.

**13. SUPPLEMENTARY NOTES** A paper submitted to the Naval War College faculty in partial satisfaction of the requirements of the Joint Military Operations Department. The contents of this paper reflect my own personal views and are not necessarily endorsed by the NWC or the Department of the Navy.

**14. ABSTRACT**

Network-Centric Warfare has demonstrated an increase in combat power using massed effects as a force multiplier. Further expansion and hardening of the Global Information Grid and the information infrastructure are needed. But to support a dispersed, collaborative force, we need to look at how the civilian world has already incorporated the concepts and exploited the netted world. This paper reviews some successful civilian uses of mass collaboration and the tools used today, as well as looking at innovative uses the military has implemented. It describes some of the shortcomings and concerns regarding command and control of a netted force, and provides recommendations on how to better integrate the tenets of mass collaboration among a decentralized force into operational design.

**15. SUBJECT TERMS**

Network Centric Warfare, NCW, collaboration, knowledge management, information management, netted force, decision superiority, information superiority, decentralized force

| 16. SECURITY CLASSIFICATION OF: | | | 17. LIMITATION OF ABSTRACT | 18. NUMBER OF PAGES | 19a. NAME OF RESPONSIBLE PERSON |
|---|---|---|---|---|---|
| a. REPORT | b. ABSTRACT | c. THIS PAGE | | | Chairman, JMO Dept |
| UNCLASSIFIED | UNCLASSIFIED | UNCLASSIFIED | | 19 | 19b. TELEPHONE NUMBER *(include area code)* 401-841-3556 |

**NAVAL WAR COLLEGE**
**Newport, R.I.**

# THE POWER OF MASS: COLLABORATION FOR A NETTED FORCE

**by**

**Nancy A. Norton**

**CAPT, USN**

**A paper submitted to the Faculty of the Naval War College in partial satisfaction of the requirements of the Department of Joint Military Operations.**

**The contents of this paper reflect my own personal views and are not necessarily endorsed by the Naval War College or the Department of the Navy.**

**Signature: _____**

**31 October 2008**

***Approved for public release; Distribution is unlimited.***

## Abstract

*The Power of Mass: Collaboration for a Netted Force*

Network-Centric Warfare has demonstrated an increase in combat power using massed effects as a force multiplier. Further expansion and hardening of the Global Information Grid and the information infrastructure are needed. But to support a dispersed, collaborative force, we need to look at how the civilian world has already incorporated the concepts and exploited the netted world. This paper reviews some successful civilian uses of mass collaboration and the tools used today, as well as looking at innovative uses the military has implemented. It describes some of the shortcomings and concerns regarding command and control of a netted force and provides recommendations on how to better integrate the tenets of mass collaboration among a decentralized force into operational design.

## Table of Contents

## INTRODUCTION

The U.S. military pioneered the concept of a fully networked force and the power to be gained from networking and collaboration, yet the rest of the world has far surpassed our ability and willingness to take advantage of this mass collaboration. The U.S. military needs to expand the focus of network centric warfare (NCW) beyond the underlying technology, and beyond the futuristic fascination with a cyber war or a technological war, to allow our military forces to gain strength through virtual massing and mass collaboration.

Network-centric warfare is less about the network than about networking the force.[1] VADM Arthur K. Cebrowski's pivotal 1998 article in *Proceedings*, "Network Centric Warfare: Its Origin and Future," states "Network Centric Warfare derives its power from the strong networking of a well-informed but geographically dispersed force."[2] The power of NCW comes from shared information and collaboration among large groups of people,[3] which creates an opportunity for increasingly decentralized and collaborative organizations.

The network was never envisioned to be the centerpiece of military operations, but was envisioned to allow the decision-maker to be central to the force networked around him. The term Decision-Centric Warfare has been proposed as a better description than Network Centric Warfare, because the purpose of a networked force is to improve decision-making.[4] However, the military has always been and will always be a decision-centric organization, whether it is networked through computer technology or through runners used to build shared awareness. A more precise term would be simply: "a netted force conducting netted

---

[1] David S. Alberts, John J. Garstka, and Frederick P. Stein, *Network Centric Warfare: Developing and Leveraging Information Superiority* (Washington DC: CCRP Publication Series, 1999), 6-7.
[2] Arthur K. Cebrowski, and John Gartska, "Network-Centric Warfare: Its Origin and Future." *U.S. Naval Institute Proceedings* 124, no. 1 (January 1998): 35.
[3] Alberts et al., *Network Centric Warfare*, 6-7.
[4] Eric P. DeLange, "Decision-Centric Warfare: Reading Between the Lines of Network-Centric Warfare." (U.S. Naval War College, Newport, RI: 2006), 15.

operations". The U.S. Navy's term for the framework of designing and funding NCW is FORCEnet, which describes a netted force, with emphasis on the FORCE, not the net.

While the information infrastructure, or "infostructure", is a fundamental enabler required to network the force,[5] it is simply the foundation upon which to build. While DoD has spent years acquiring and fielding the infostructure through various joint and Service programs, it has put much less emphasis on the people, processes, policies, training and organizational changes required to produce true transformational capabilities for netted forces.[6] In the meantime, the civilian world, stimulated by both business and social uses, has learned how to gain power in decentralized organizations using mass collaboration to reach out to the edges of a netted world.

This paper will begin with a review of the concepts of network centric warfare and how they relate to military operations and operational art. Then it will look at how the business world has exploited the benefits of collaborating in a netted world, how those same capabilities have been adapted for broad personal use, and provide examples of military adaptations. Next, the paper will look at potential concerns and shortfalls of collaboration across a netted military force. Finally, the paper will conclude with recommendations regarding broader implementation and integration into operational design and execution.

## BACKGROUND

Network-centric warfare is defined as "an information superiority-enabled concept of operations that generates increased combat power by networking sensors, decision makers, and shooters to achieve shared awareness, increased speed of command, higher tempo of operations, greater lethality, increased survivability, and a degree of self-synchronization. In

[5] Alberts et al., *Network Centric Warfare*, 6.
[6] David S. Alberts, *Information Age Transformation* (Washington, DC: CCRP Publication Series, 2002), 17.

essence, NCW translates information superiority into combat power by effectively linking knowledgeable entities in the battlespace."[7] Figure 1 represents this definition, which supports an operational concept of massing effects rather than massing forces,[8] with a smaller force in the battlespace, and much of the rear support forces widely dispersed.

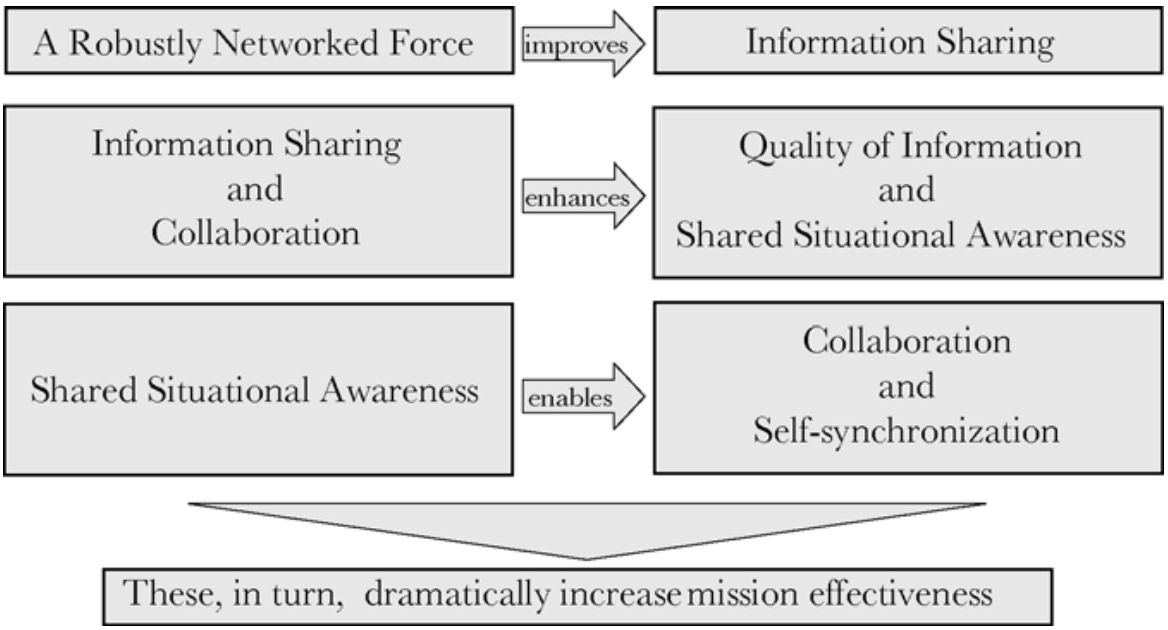


**Figure 1. The Tenets of NCW** (reprinted from David S. Alberts and Richard E. Hayes, *Power to the Edge: Command and Control in the Information Age*, (Washington, DC: CCRP Publication Series, 2003), 108.)

This movement towards collaboration and a self-synchronized force proceeds through steps of maturity in NCW as displayed in Figure 2. Each step requires improvements to "the entry fee" of a robust, secure, integrated, and interoperable infostructure consisting of a global information grid (GIG), computing power, applications and display tools designed to promote maximum shared awareness in a decision-centric organization.[9]

[7] Alberts et al., *Network Centric Warfare*, 2.
[8] Ibid, 88.
[9] Ibid, 35.

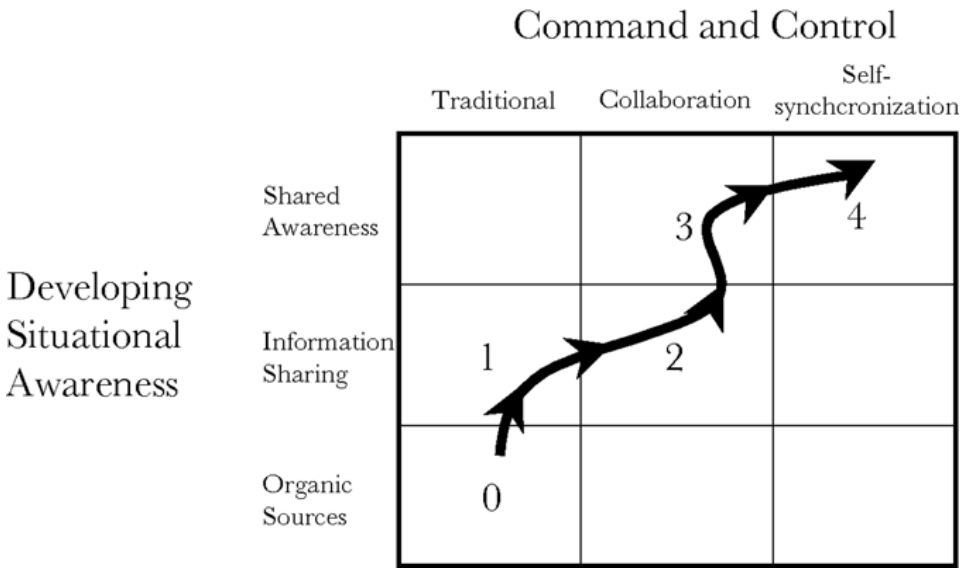


**Figure 2. NCW Maturity Model** (reprinted from David S. Alberts and Richard E. Hayes, *Power to the Edge: Command and Control in the Information Age*, (Washington, DC: CCRP Publication Series, 2003), 109.)

Much of the DoD focus to date has been on building the infostructure required to network the force, often without developing the equally important concepts of operation, processes, doctrine, and training required to take advantage of the growing capability for shared awareness to enable collaboration and self-synchronization. Additionally, a move towards embracing the true concepts of NCW, and gaining the advantages of a netted force, rather than just a focus on technology, will require new organizational and operational art constructs with a more decentralized approach at all levels from strategic to tactical.[10]

## DISCUSSION

The military of today is living in a world that has embraced mass collaboration and the value it provides. While DoD has focused on incremental improvements to the infostructure, the world has transformed through mass collaboration. With a 300% increase in world-wide internet usage from 2000 to 2008, the internet has become the robust, fully-networked grid required to reach across much of the world, with approximately 21% of the

[10] Alberts et al., *Network Centric Warfare*, 85.

world population connected.[11] With that comes access to information, allowing participation in the economy and production process as never before. The availability of a low-cost collaborative environment is changing processes and organizations across industries.[12] The shift from a rigid, centralized commercial organization to a flexible, decentralized organizational structure seems almost inevitable, whether in legitimate organizations or not.

Decentralization has been the key to the success of peer-to-peer music sharing, with incredibly damaging effects on the legitimate recording industry. From Napster to Kazaa to eMule, the record industry has fought increasingly decentralized, self-synchronizing groups collaborating over the internet with a common goal – to reduce the cost of listening to their favorite music. Trying to defeat music sharing groups has cost much of the industry's traditional profits and has made each replacement group even more decentralized.[13]

Adaptive traditional businesses have recognized the phenomenon of collaboration and have chosen to exploit the concepts rather than try to fight them. Global companies have recognized that they can use collaboration and a networked environment to shift work to follow the sun, resulting in a competitive advantage for the entire organization.[14] They have also become more decentralized. Under Jack Welch, GE set up independently accountable business units, giving the company greater flexibility in each individual market, and significantly improving their market value.[15]

Other companies have taken this decentralized approach from conception, and to a much larger scale. The internet infostructure has enabled anyone to become a retailer through the use of the mass collaboration sales website eBay. It is a decentralized organization which

[11] Internet Usage Statistics, http://www.internetworldstats.com/stats.htm (accessed 19 October 2008).
[12] Don Tapscott, and Anthony D. Williams, *Wikinomics* (New York: Penguin Group, 2008), 10-11.
[13] Ori Brafman, and Rod A. Beckstrom, *The Starfish and the Spider* (New York: Penguin Group, 2006), 21-27.
[14] Alberts et al., *Network Centric Warfare*, 39.
[15] Brafman and Beckstrom, *Starfish and the Spider*, 175.

is flexible and agile enough to respond to the market quickly. eBay was designed with incredible individual capability and trust, and has created limiting policies only when necessary and only for critical processes. For example, as the business grew in popularity and use, eBay bought PayPal in recognition of the need for structure and security around monetary transactions to bolster trust and confidence.[16]

Mass collaboration in personal use has exploded even more rapidly than in business use. There are numerous examples of mass collaboration sites which are widely and frequently used primarily for social interaction, such as Facebook, MySpace, and Twitter. LinkedIn and Biznik collaboration sites are used primarily for business-related interactions. Still others have crossed both social networking and business networking, with a very broad base of users and functions, including their own virtual commerce earning real money, such as Second Life. These sites have hundreds of thousands of users who combine physical and virtual relationships through mass collaboration tools.[17]

The capability to collaborate has created a new concept of production through collaboration. The Linux open operating system was the first significant example of a product which was given to its users to improve. Programmers around the world have become peer producers, modifying the software to improve its performance, while freely sharing the updated software.[18] Both IBM and Sun now provide free open-source software that is improved continuously through corporate and volunteer collaboration.[19]

Wikipedia was created when a hierarchical process to review and publish user submitted information for an online encyclopedia failed. In its place came an encyclopedia

[16] Brafman and Beckstrom, *Starfish and the Spider*, 163-166.
[17] Tapscott and Williams, *Wikinomics*, 125.
[18] Ibid, 23-24.
[19] Brafman and Beckstrom, *Starfish and the Spider*, 172-173.

built on Wiki collaboration software which allows users to create their own content directly.[20] It has become one of the most significant and most popular examples of collaborative user production to date. With just five full time employees, and on-line volunteers who monitor content, more than one hundred thousand regular contributors collaborate and self-correct over ten times the data found in *Encyclopedia Britannica*.[21]

Other examples of user production through mass collaboration include videos on YouTube, and pictures shared on Flickr and linked to positions on Google Earth. Each of these sites has flourished, with virtually no centralized structure or direct profit motive. Peer production is successful largely because people have a desire to contribute based on their expertise and experiences.[22] Self-selection allows people to contribute in areas of their own interest, where they choose to work on tasks they are uniquely qualified to perform.[23]

The ease of quickly retrieving data of individual interest drives the popularity of these websites. The network and simple software applications allow each user to define their search criteria and the types of websites they choose to visit, which reduces volumes of data on any subject down to the information of immediate interest. These tools encourage further innovative applications for increased collaboration.

Collaboration is already a part of military processes, although to a much less dramatic degree than the previous public examples. The Common Operational Picture (COP) is an example of mass collaboration that has improved over many years. More participants in the battlespace are becoming connected nodes, providing a more densely netted force, with the ability to quickly and broadly share the common picture. Each sensor node has the ability to

[20] Tapscott and Williams, *Wikinomics*, 72-73.
[21] Ibid, 12-13.
[22] Brafman and Beckstrom, *Starfish and the Spider*, 74.
[23] Tapscott and Williams, *Wikinomics*, 68-70.

contribute some type of information, even if only their own position. Knowledgeable sensors or human nodes can contribute more useful information and share a picture that is richer (higher quality) and has greater reach (spread throughout the network).[24] This picture is now shared between strategic, operational, and tactical levels, moving DoD up in the NCW Maturity Model shown in Figure 2 from 0 to 2.

Chat has transformed how geographically dispersed military units communicate. This simple internet-based tool provides the ability to rapidly share planning and operational data between units in near real-time. Chat rooms have not simply replaced communications over once-crowded voice circuits, they have fostered entirely new processes that are functionally based and often self-synchronized, to conduct strike operations, distance support for logistics and maintenance, and planning coordination. They have become virtual organizations, able to accomplish tasks without regard to location.[25] The infostructure of the GIG has provided the connectivity and bandwidth required for units and individuals to become nodes with shared awareness of their environment, moving DoD into NCW Maturity Model levels 3 and 4.

During the early days of Operation ENDURING FREEDOM, TASK FORCE 50 successfully used collaborative tools for peer production, which was integrated into their normal operations and organization structure. Prior to deploying, the Commander developed an operational vision and leadership style that directed a collaborative, decentralized approach to operations. Using the Knowledge Wall and Knowledge Web or KWeb, the TASK FORCE 50 staff was able to replace the Commander's morning brief with a more efficient, living display of relevant operational data, shared with the other U.S. ships in the

[24] Paul T. Mitchell, *Network Centric Warfare: Coalition Operations in the Age of U.S. Military Primacy*. (London: The International Institute for Strategic Studies, 2006), 34.
[25] Alberts et al., *Network Centric Warfare*, 35.

theater. The Commander was able to hold much shorter meetings, focused on areas of concern, which freed up time for the staff to invest in critical planning functions.[26]

Since 2001, joint and coalition commanders have expanded the use of horizontal and vertical collaboration tools across their dispersed forces for coordinating planning and operations, including IRAQI FREEDOM. Metcalf's Law asserts that the value of a network grows exponentially with the linear growth in the number of nodes on the network.[27] The recent growth in networking ground and maritime forces, together with manned and unmanned air vehicles, all as information sharing nodes, has increased shared awareness and operational effectiveness and supported Metcalf's Law. The Navy's Maritime Headquarters with Maritime Operations Center (MHQ w/MOC) will require all of the MOCs to be fully networked nodes with shared awareness. We will see an even more rapid expansion of network nodes as unmanned aerial vehicles proliferate and ground and maritime robots become smaller and cheaper until they can be deployed in large numbers and begin to take on the behavior of highly specialized swarms that can work together to complete complex tasks and provide an even more robust sensor grid.[28]

## CONCLUSIONS

Those entering the military today and in the future will not know a life without mass collaboration, either in business or their personal lives. A fully netted military force has great potential to use these concepts and capabilities to gain knowledge and decision superiority and increase combat power and operational effectiveness. The infostructure and tools

[26] Mark Adkins, and John Kruse, *Case Study: Network Centric Warfare in the U.S. Navy's Fifth Fleet* (Tucson, AZ: University of Arizona, 2003). http://www.oft.osd.mil/initiatives/ncw/docs/CTF50_NCW_Case_Study.pdf (accessed 20 October 2008), 29.
[27] Alberts et al., *Network Centric Warfare*, 29.
[28] David S. Alberts, and Richard E. Hayes, *Power to the Edge: Command and Control in the Information Age.* (Washington, DC: CCRP Publication Series, 2003), 169.

available to our military today are sufficient to enable peer production of a richer shared operating picture, and create virtual collaborative teams to conduct shared planning and integrated operations distributed across the globe.

The richest information in a unit is typically at its edges, the tactical edge for military forces.[29] A highly informed, decision-centric organization is able to spread distinct and rich knowledge from the edges to the decision-maker. More knowledgeable decision-makers have the ability to approach problems in new ways.[30] A collaborative force that self-synchronizes and shares knowledge between edge entities can decentralize the very process of decision-making and allow the edges to act on their shared awareness directly. Successfully integrating joint fires is an example being used today. DoD's collaborative information environment (CIE) toolset is already expansive. However, no single tool or suite of tools satisfies all users, and each tool only collaborates with other users on the same system.

Much of the opposition to NCW reflects the same concern regarding a focus on technology and the network, at the expense of the people and processes, as previously described in this paper. The thought that "technology should be used not as a master but as a tool to make the decision-making process faster and more effective"[31] is correct, and is supported by the preponderance of NCW literature, and most operational commanders.

However, there are important risks and drawbacks associated with a netted force to consider. The limitations of force connectedness, interoperability, and continuity, the need to prevent information overload, and the unintended consequences of netted warfare are all real concerns to be addressed and managed.

[29] Brafman and Beckstrom. *Starfish and the Spider*, 204.
[30] Alberts et al., *Network Centric Warfare*, 149.
[31] Milan Vego, *Joint Operational Warfare* (Newport, RI: U.S. Naval War College, 2007), IX-55.

Today's reality is that everyone cannot be part of the netted force. There are limitations to networking due to laws of physics and affordability which preclude connecting all forces regardless of time, location or mission. The sensor grid is being expanded by the Services and agencies, to support ISR, fires, logistics, air and maritime domain awareness, blue force tracking, communications, and more. But not all forces are connected.

Regardless of who the military is working with, whether units from another region, joint forces, coalition countries, or non-traditional partners such as interagency (IA), inter- and non-governmental organizations (IGOs and NGOs), interoperability of networks and applications will continue to be one of the most difficult and important obstacles to overcome. Technology may prevent interoperability, but more often there are complex and bureaucratic information releasability restrictions to overcome. These will require a combination of complex and expensive technological changes, policy or law modifications, and elaborate process adjustments. If interoperability cannot be improved, the ratio of disconnected forces, lacking shared awareness, will remain unacceptably high.

The success of connecting the military raises its own major concern regarding DoD's reliance on the network. A fully netted force is a critical capability for the U.S. military, and as such, has become a critical vulnerability. If DoD continues to substitute mass force with mass effects through the use of NCW, a loss of network connectivity through enemy, friendly or neutral actions can leave an operational commander without the forces required to meet his objective. DoD has to prepare for an attack aimed at this vulnerability.

The ability of the human mind to process vast amounts of information may become the limiting factor in netted warfare. Many already complain that information overload is more detrimental than a lack of information.

The unintended consequences of a fully netted force include some of the concepts that generate the most visceral opposition to NCW. The two extremes of this concern are micromanagement and loss of control. Technology doesn't cause micromanagement, but it has increasingly enabled those who choose to micromanage their forces. Micromanagement can result from any increase in the ability of a commander to see and directly influence the actions of his forces without going through the layers of the organization. There is a real need to limit micromanagement, but it is best dealt with as a problem of leadership and operational art, not a problem of netted warfare.

On the other extreme, some commanders worry that they will lose control of their organizations as the reach of knowledge spreads to the edge of their forces. Some worry that decentralizing knowledge will automatically result in inappropriate decisions being made by people not authorized to make them. Others think that more knowledgeable forces will have a greater tendency to second-guess the decisions of the commander. Again, these tendencies are enabled by technology, but not caused by it. Commanders have always had a requirement to give direction and limitations to their forces regarding their authority to act, in battle and in planning. Rules of engagement, standing orders, tactics, techniques and procedures, qualifications, designations, and delegation of authorities are all required to simultaneously encourage and restrict action and decision making beyond the commander. Each commander must communicate their vision and intent in order to build the trust of his forces.

Allowing flexibility in the organization structure and increasing information sharing across units would produce a more decentralized military, with a distribution of knowledge and power down to the lowest levels, or out to the edge of the organization.[32] This should result in a more agile force, better able to respond rapidly and to benefit from diverse

[32] Alberts and Hayes, *Power to the Edge*, 185.

perspectives.[33] However, this is not the type of organizational structure that the military is typically comfortable with. There are concerns that a flatter military organization will be less effective and more difficult to command.

## RECOMMENDATIONS

The vision of a fully netted force can only be achieved through strong leadership. Military leaders need to either promote it as an operational concept, or step out of the way and allow a decentralized and unstructured approach to innovation and process change. DoD needs to increase funding and encourage innovative solutions to improving every aspect of sense-making for the data it currently has, and could become overwhelmed by. There is common recognition that a COP is useful, but a User Defined Operational Picture (UDOP) or Common Relevant Operational Picture (CROP) would be more useful tailored to each mission. A better way to limit information overload is needed, such as "valued information at the right time", or VIRT. Computers can be configured to limit data passed to consumers based on their defined "conditions of interest", or COI. This becomes a smart-push system to monitor routine information and allow the operator to respond to alerts of important elements of interest or unpredictable events. There are commercial examples of this, such as choosing movies to order on Netflix.[34] Netflix recommends movies that are similar to those viewed and enjoyed in the past, and the filtering continuously improves based on further user inputs.

Military forces require effective, user-friendly, and flexible display tools. The idea that a picture is worth a thousand words should be incorporated through the development of filtering, sorting, processing, and fusing of data into functional displays of knowledge, aimed

[33] Alberts and Hayes, *Power to the Edge*, 217.
[34] Frederick Hayes-Roth, "Valued Information at the Right Time (VIRT): Why Less Volume is More Value in Hastily Formed Networks", (Naval Postgraduate School, Monterey, CA, 2006), http://www.nps.edu/cebrowski/Docs/VIRTforHFNs.pdf (accessed 24 October 2008), 3-5.

at improved decision-making. Data that may have once seemed impossible to process in a timely manner is transformed into usable data when fused and displayed properly.[35] A pilot would find it very difficult to navigate a long and indirect route if required to use just a long list of latitude and longitude points. If given a navigational chart with those same points mapped out and the ability to navigate visually, the same task becomes much easier. With waypoints loaded in a navigation system, the task becomes almost trivial. Similarly, deconflicting maneuvering forces using just numerical position locations is difficult and slow. But that same task can be made simple with visual displays of forces on a shared operational picture. Given the right manner of display, a vast amount of information can be absorbed and understood very quickly.

As the sensor grid continues to grow, DoD needs to become even more mindful of the need for interoperability and data fusion. Without using common data standards and protocols, proprietary data formats could create stovepipes of information, such as tracking devices that can only be used in logistics systems, even when needed in an air or maritime awareness picture. Just as Google has the ability to provide layers of disparate data on maps with imagery, restaurants, mass transit routes, user-provided pictures, and real-time GPS positions of your friends from their cell phones just to plan a lunch date, the military needs to be able to mix and match the most useful data available to an individual at any given time, regardless of the source.

Artificial stovepipes for information sharing are created within different CIEs directed by Services or combatant commanders, limiting collaboration and innovation where it is most needed - between joint organizations. DoD needs to narrow the choice of collaboration tool suites to just a few, and promote their use and proficiency. Then it should

[35] Vego, *Joint Operational Warfare*, XIII-7.

create a demand signal with industry for collaboration suites that are able to connect with users on other systems. Just as users with cell phones on AT&T's network can talk to users on the Sprint network, users on an Information Work Space (IWS) suite should be able to seamlessly collaborate with users of Adobe Connect.

DoD needs to continue building a robust infostructure out to the disconnected users as funding and technology allow, and regularly upgrade those minimally connected forces to provide increased network access, data security, and continuity of operations. But since DoD can't afford to have the entire force fully netted, widespread process reengineering must be considered carefully, with secondary processes designed to accommodate the disconnected.

Improvements to the infostructure need to be accelerated in two critical areas: multinational information sharing and information security. While these are often seen as opposing forces, they are both key requirements to achieving a fully netted force. Current and future military operations require working with multinational, IA, NGO, and IGO participants. DoD cannot afford to minimize the contributions of these organizations because its networks cannot connect or data cannot be shared. Non-traditional partners are often the knowledgeable edge with the richest information to share. But information sharing cannot be achieved at the expense of information security. As DoD networks and the netted warfare processes have become a critical strength, they have also become more vulnerable to denial, disruption, destruction, and exploitation. As the network has expanded, the potential threat of a malicious insider has also grown. Additional capabilities are required to protect the networks and the data riding on them in order to minimize this critical vulnerability.

The most important recommendations are those relating to the human aspects of a fully netted force, because they tend to be overlooked. As was stated in the 2001 Network

Centric Warfare Report to Congress, "Networking the Force entails much more than providing connectivity among force components in the physical domain. It involves the development of doctrine and associated tactics, techniques, and procedures that enable a force to develop and leverage an information advantage to increase combat power."[36] Every possible opportunity should be seized to train on collaborative tools, techniques, and processes, integrated into operational design, while considering the potential problems of commanding a netted force. Joint and multinational exercises, experimentation, and joint professional military education should lead the promotion of a netted force. All DoD operational planning courses, for all ranks, should be taught using the collaboration systems that are common in the field.

Organizational changes should be encouraged and studied to learn how to capture the positive results of a decentralized organization while minimizing concerns. Concerns that it will be less effective and more difficult to command must be addressed. Business has recognized that the ability to manage the skills of dispersed organizations and people is becoming an essential skill.[37] The military must recognize this change as well.

The Navy's MHQ w/MOC will enable a collaborative, decentralized structure. With training and practice, these netted MOCs will create virtual teams to distribute work across geographical theaters, and allow the Navy to use the best available expertise to solve complex problems. If the commanders will integrate netted concepts into their operational design to encourage innovation and an adaptive organizational structure, the MOC could be a real-world lab, testing and demonstrating the power of mass collaboration.

---

[36] U.S. Department of Defense, *Network Centric Warfare Department of Defense Report to Congress* (Washington, DC: Department of Defense, July 2001). http://www.dodccrp.org/research/ncw/ncw_report/report/ncw_cover.html (accessed 6 September 2008). 3-1.
[37] Tapscott and Williams, *Wikinomics*, 18.

Implementing the tenets of NCW, mass collaboration, and the ensuing decentralization of knowledge and power comes with risk. But ignoring the benefits to be gained through military forces with a shared awareness comes at a much greater risk. The expansion of the netted world is making an increasingly collaborative force inevitable and perhaps even less threatening. Commanders must have the vision to shape and guide this inevitable shift so that it can become a fundamental part of operational art to embrace and exploit, rather than just a technological change to fear and avoid.

## BIBLIOGRAPHY


Adkins, Mark, and John Kruse. *Case Study: Network Centric Warfare in the U.S. Navy's Fifth Fleet*. Arizona: University of Arizona, August 2003. http://www.oft.osd.mil/initiatives/ncw/docs/CTF50_NCW_Case_Study.pdf (accessed 20 October 2008).

Alberts, David S., John J. Gartska, and Frederick P. Stein. *Network Centric Warfare: Developing and Leveraging Information Superiority*. Washington, DC: CCRP Publication Series, 1999.

Alberts, David S. *Information Age Transformation.* Washington, DC: CCRP Publication Series, 2002.

Alberts, David S., and Richard E. Hayes. *Power to the Edge: Command and Control in the Information Age.* Washington, DC: CCRP Publication Series, 2003.

Alberts, David S., and Richard E. Hayes. *Campaigns of Experimentation: Pathways to Innovation and Transformation.* Washington, DC: CCRP Publication Series, 2005.

Barnett, Thomas P.M. "The Seven Deadly Sins of Network-Centric Warfare." *U.S. Naval Institute Proceedings* 125, no. 1 (January 1999): 36-39.

Brafman, Ori and Rod A. Beckstrom. *The Starfish and the Spider*. New York: Penguin Group, 2006.

Cebrowski, Arthur K. and John Gartska. "Network-Centric Warfare: Its Origin and Future." *U.S. Naval Institute Proceedings* 124, no. 1 (January 1998): 28-35.

Clarkson, Jeffrey, Jeffrey Grossman, Jay Martin and Paul Shigley. "Composeable FORCEnet Becomes Reality." *U.S. Naval Institute Proceedings* 133, no. 10 (October 2007): 71-74.

DeLange, Eric P. "Decision-Centric Warfare: Reading Between the Lines of Network-Centric Warfare." Research paper, Newport, RI: U.S. Naval War College, 2006.

Hayes-Roth, Frederick. "Valued Information at the Right Time (VIRT): Why Less Volume is More Value in Hastily Formed Networks", Monterey, CA: Naval Postgraduate School, 2006. http://www.nps.edu/cebrowski/Docs/VIRTforHFNs.pdf (accessed 24 October 2008).

Internet World Stats. "Internet Usage Statistics." http://www.internetworldstats.com/stats.htm (accessed 19 October 2008).

Kuzmick, James J. "It's Not Just the Information – It's the Correlation." *U.S. Naval Institute Proceeding*, 131, no. 2 (February 2005): 46-49.

Luddy, John. *The Challenge and Promise of Network-Centric Warfare*. Arlington, VA: Lexington Institute, February 2005.

Mitchell, Paul T. *Network Centric Warfare: Coalition Operations in the Age of U.S. Military Primacy*. London: The International Institute for Strategic Studies, 2006.

Moffat, James. *Complexity Theory and Network Centric Warfare*. Washington, DC: CCRP Publication Series, 2003.

Tapscott, Don, and Anthony D. Williams. *Wikinomics.* New York: Penguin Group, 2008.

Tomaszeski, Steven J. "Heart of ForceNet: Sensor Grid, Advanced Command and Control." *Sea Power*, (March 2004): 14-16.

U.S. Department of Defense. *Network Centric Warfare Department of Defense Report to Congress.* Washington, DC: Department of Defense, July 2001. http://www.dodccrp.org/research/ncw/ncw_report/report/ncw_cover.html (accessed 6 September 2008).

U.S. Department of Defense Office of Force Transformation. *The Implementation of Network-Centric Warfare.* Washington, DC: January 2005.

U.S. Office of the Chairman of the Joint Chiefs of Staff. *Information Operations*. Joint Publication (JP) 3-13. Washington, DC: CJCS, 13 February 2006.

U.S. Office of the Chairman of the Joint Chiefs of Staff. *Joint Communications Systems*, Joint Publication (JP) 6-0. Washington, DC: CJCS, 20 March 2006.

U.S. Office of the Chairman of the Joint Chiefs of Staff. *Joint Vision 2020*. Washington, D.C: CJCS, 2000.

U.S. President. *National Strategy for Information Sharing*. Washington, DC: White House, October 2007.

Vego, Milan. *Joint Operational Warfare*. Newport, RI: U.S. Naval War College, 2007.